ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

УДК 004.056

В. Ю. Корольов, к. т. н.;

В. В. Поліновський;

В. А. Герасименко

RS-СТЕГАНОАНАЛІЗ. ПРИНЦИПИ РОБОТИ, НЕДОЛІКИ ТА КОНЦЕПЦІЯ МЕТОДУ ЙОГО ОБХОДУ

Подано алгоритм RS-стеганоаналізу, наведено його переваги, а також показано недоліки, які дозволяють уникнути виявлення прихованих повідомлень. Запропоновано концепцію побудови нового методу стеганографічного приховування інформації, яка не виявляється RS-стеганоаналізом.

Вступ

Сучасна комп'ютерна стеганографія набуває потужнішого розвитку — принципи стеганографічного приховування інформації в поєднанні з методами криптографії є базою для створення сучасних технологій захисту інформації, а також комп'ютерної безпеки і пристроїв персоналізації [1] як для корпоративного застосування, так і для особистого використання.

Стеганографічний підхід до захисту інформації [2—5] відрізняється від криптографічного, метою якого є зробити комунікації нерозбірливими для всіх, хто не має ключів шифрування. Засоби стеганографії використовують психосенсорну релевантність мультимедійних файлів для приховування не тільки секретного повідомлення, але і факту його передачі. У прикладних програмних продуктах методи стеганографічного захисту даних вже не використовуються окремо, а тільки після шифрування конфіденційної інформації криптографічними методами. Тому розробка нових стегано-криптографічних методів захисту інформації є актуальною науково-практичною задачею.

Аналіз стану проблеми та постановка задачі

Більшість комерційних стеганографічних програмних продуктів використовують вбудовування стего-бітів у НЗ рівень контейнера для приховування даних у кольорових і монохромних зображеннях. Розробники програмних додатків виходять з припущення, що зміни в НЗБ кольорів не можуть бути виявлені, оскільки шум реєстрації цифрових зображень маскуватиме вбудовані стего-біти.

У стеганографії чим менше інформації у контейнері, тим менша імовірність того, що вбудоване у стего-образ повідомлення буде виявлене за артефактами. Вибір контейнера особою, яка відправляє повідомлення, також визначає, наскільки легко існування секретного повідомлення може бути розкрито. Зображень з невеликою кількістю кольорів, комп'ютерного мистецтва, зображень з унікальним змістом, таких як шрифти, слід уникати у використанні в якості контейнерів. Натомість неархівовані і неформатовані фотографії, перетворені у цифрову форму сканерами, та зображення, отримані цифровими фотокамерами, містять багато кольорів. Тому вони зазвичай розглядаються як безпечні для стеганографії.

Зображення у популярному форматі JPEG є поганими контейнерами для використання стеганографічних методів. JPEG-квантування залишає на зображенні унікальний шаблон, аналіз якого дозволяє виявити малі модифікації контейнера, викликані стего-бітами [6].

Наразі активно розвиваються методи, алгоритми та процедури виявлення факту вбудовування в контейнер стего-біт і оцінка розміру прихованого повідомлення — стегано-аналіз.

Метою роботи є дослідження алгоритму RS-стеганоаналізу з виявлення прихованих повідомлень у зображеннях доступних у мережі Інтернет, а також вивчення його недоліків та перевірки можливостей пасивної протидії цьому алгоритму.

Концепція RS-аналізу

Для більшості зображень НЗБ-рівень вважається випадковим, оскільки він не містить будь-якої структури, що легко розпізнається. Проте, НЗБ-рівень, навіть якщо виглядає випадковим, є разом з тим пов'язаним з іншими бітовими рівнями нелінійною залежністю, на чому і ґрунтується RS-стеганоаналіз. Тому класичні статистичні характеристики й оцінки, застосовані до НЗБ-рівня, не можуть надійно визначити ступінь його випадковості.

Проте, *RS*-аналіз може легко виявити повідомлення, вбудовані у цей клас зображень і досить точно оцінити довжину повідомлень. Аналіз відмінностей у НЗБ-площини і зсунутої НЗБ-площини стего-образу дозволяє надійно виявляти повідомлення розміром від 1 % і більше від загальної кількості пікселів (1 біт на відлік). Крім того, для RS-аналізу можна побудувати швидкий алгоритм.

У відповідності до реалізації винаходу метод виявлення НЗБ вбудованого прихованого повідомлення, відліки якого випадково розміщені в площині контейнера, складається з таких кроків [6—8]:

1. Розділення стего-образу на групи сусідніх відліків, які не мають спільних елементів;
2. Обчислення дискримінаційної функції для кожної групи;
3. Виконання над групами переставних операцій для визначення обернено-збурених груп пікселів;
4. Віднесення груп відліків за результатом переставних операцій до класів: регулярні (*R*), сингулярні (*S*), невикористані (*U*);
5. Нанесення на *RS*-діаграму значень для *R* і *S* груп стего-образу;
6. Побудова кривих *RS*-діаграми й обчислення їхнього перетину за екстраполяцією.
7. Визначення існування або не існування секретного повідомлення за їхнім перетином;
8. Розрахунок довжини повідомлення за координатами перетину кривих.

Нехай контейнер — це зображення розміром $M\times$N пікселів і значеннями пікселів з множини P. Наприклад, для 8-бітного монохромного зображення $P = \{0, 1,\ldots, 255\}$. Аналіз стего-образу починається з ділення зображення на групи з n суміжних пікселів $(x_1, x_2, \ldots, x_n)$ без перетину елементів. У алгоритмі вибирають групи з n послідовних пікселів у рядку. Далі визначається дискримінаційна функція f, за якою для кожної групи $G = (x_1, x_2, \ldots, x_n)$ розраховується дійсне число $f(x_1, x_2, \ldots, x_n) \in R$. Значення дискримінаційної функції визначає регулярність (гладкість) групи G пікселів. Чим більше шуму у елементах групи, тим менше значення дискримінаційної функції.

Задамо дискримінаційну функцію f, за якою будемо оцінювати «варіації» групи G

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n-1} \left|x_{i+1} - x_i\right|. \qquad (1)$$

Можна побудувати іншу дискримінаційну функцію на базі статистичних моделей або апріорної інформації про контейнер.

Задаємо операцію обернення F на P, яку називають «перевертання». Перевертання — це перестановка рівнів відтінків сірого, який складається з двох циклів і має властивість таку, що $F^2 =$ Identity або $F(F(x)) = x$, для всіх $x \in P$.

Перестановка F_1: $0 \ll 1, 2 \ll 3, \ldots, 254 \ll 255$ відповідає зменшенню НЗБ кожного сірого рівня. Далі задаємо зсунуте НЗБ перевертання F_{-1} як $1 \ll 2, 3 \ll 4, \ldots, 253 \ll 254$ або $F_{-1} = F_1(x + 1) - 1$ для всіх x.

Для повноти ми також визначаємо F_0 як тотожну перестановку $F(x)$ для всіх $x \in P$. Використовуючи дискримінаційну функцію F, виділяємо три групи пікселів [8]:

— регулярні групи $G \in R \Leftrightarrow f\left(F\left(G\right)\right) > f\left(G\right)$;

— сингулярні групи $G \in S \Leftrightarrow f\left(F\left(G\right)\right) < f\left(G\right)$;

— невикористані групи $G \in U \Leftrightarrow f\left(F\left(G\right)\right) = f\left(G\right)$.

Позначення $F(G)$ означає, операція перевертання F застосована до всіх компонент вектора G. Можливі і інші варіанти перевертання до компонент вектора G. Операція перевертання вектора може бути виражена за допомогою маски M, яка називається n-кортежем зі значеннями −1, 0 і 1. Перевернута група $F(G)$ визначається як $F_{M(1)}(X_1)$, $F_{M(2)}(X_2),...,F_{M(n)}(X_n)$.

Метою застосування перевертальної функції F є збурення малої кількості значень пікселів зворотним способом, чим симулюється дія НЗБ-стеганографічного алгоритму. Для типових зображень додавання невеликої кількості шуму (перевертання малої кількості значень) призведе швидше до збільшення значення дискримінаційної функції. Тобто загальна кількість регулярних груп (R) буде більшою, ніж кількість сингулярних груп (S).

Позначимо кількість регулярних груп для маски M як R_M (у відсотках від усіх груп). Аналогічно S_M позначимо відносну кількість сингулярних груп. Маємо $R_M + S_M \le 1$ для позитивної маски і $R_{-M} + S_{-M} \le 1$ для негативної маски. Статистичні гіпотези стеганоаналітичної методики полягають у тому, що в типовому зображенні очікуване значення R_M дорівнює R_{-M} і те саме вірно для S_M і S_{-M}:

$$R_M \approx R_{-M} \text{ і } S_M \approx S_{-M}. \qquad (2)$$

Ця гіпотеза може бути евристично перевірена аналізом залежності (1).

Перевертальна операція F_{-1}, як і F_1 застосовується до зображення, кольори якого були зсунуті на одиницю. Для типового зображення не існує апріорної причини, чому кількість R і S груп повинна суттєво відрізнятись у разі зсуву кольорів на одиницю.

Автори винаходу переконані, що мають вичерпні експериментальні докази того, що гіпотеза (2) виконується дуже точно для зображень, отриманих з цифрових камер, як для форматів з втратами, так і для форматів без втрат. Це також добре витримується для зображень, оброблених звичайними операціями, і для більшості сканованих зображень. Проте відношення (2) порушується, якщо НЗБ-рівень рандомізовано, наприклад, НЗБ-стеганографією.

Рандомізація НЗБ-рівня спрямовує різницю між R_M і S_M до нуля, з ростом довжини m повідомлення. Після перевертання НЗБ-рівня 50 % пікселів (що буде після вбудовування біта шифрованого повідомлення в кожен піксел) ми отримаємо $R_M \approx S_M$.

Цікаво, що рандомізація НЗБ-рівня має протилежний вплив на R_{-M} і S_{-M}. Їх різниця збільшується зі зростанням довжини m вбудованого повідомлення. Просте пояснення збільшення різниці між R_{-M} і S_{-M} може бути запропоновано для маски $M = [0; 1; 1; 0]$. Означимо: множину $C_i = \{2i, 2i + 1\}$, $i = 0,1,\ldots,127$ і

множину груп $C_{rst} = \{G | G \in C_r \times C_s \times C_t\}$.

Існує 128^3 замкнутих множин, кожна з яких складається з 8 груп (триплетів). Для цілей аналізу було обрано чотири різних типи множин, ігноруючи ті, що горизонтально і вертикально симетричні. У табл. 1. подано ці чотири типи і кількість R, S і U груп після F_1 F_{-1} для кожного типу. З табл. 1 видно, що рандомізація НЗБ намагається вирівняти кількість R і S груп в кожній підмножині після F_1, тоді як кількість R груп зростає, кількість S груп спадає після F_{-1}.

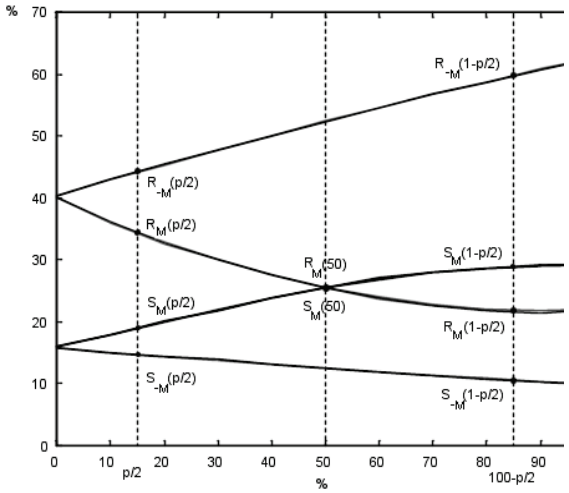
Таблиця 1

Кількість *R* і *S* груп після перевертання першого і другого етапів

Тип множини	F_1 перевертання	F_{-1} перевертання
$r = s = t$	$2R, 2S, 4U$	$8R$
$r = s > t$	$2R, 2S, 4U$	$4R, 4U$
$r < s > t$	$4R, 4S$	$4R, 4S$
$r > s < t$	$8U$	$8U$

RS стеганоаналітична методика подана у винаході, оцінює чотири криві *RS*-діаграми й обчислює їхній перетин за екстраполяцією. Загальна форма чотирьох кривих на діаграмі змінюється в залежності від контейнера (рис. 1) від практично ідеально лінійної до кривої. Експерименти показали, що R_{-M} S_{-M} добре апроксимуються прямими лініями; внутрішні криві R_M і S_M достатньо добре апроксимуються поліномами другого порядку.

Для стего-образу з повідомленням невідомої довжини p (у процентах від кількості пікселів), яке вбудоване НЗБ пікселів і випадково розміщене у площині, початкові вимірювання кількості R і S груп відповідають точкам $R_M(p/2)$, $SM(p/2)$, $R_{-M}(p/2)$ і $S_{-M}(p/2)$. Ділення на два отримуємо з того факту, що для випадкового повідомлення приблизно половина пікселів буде перевернута. Якщо ми перевернемо НЗБ-ти всіх пікселів зображення і порахуємо кількість R і S груп, то можемо отримати чотири точки $R_M(1-p/2)$, $S_M(1-p/2)$, $R_{-M}(1-p/2)$, $S_{-M}(1-p/2)$.



RS-діаграма

Через точки можна провести прямі лінії $R_M(p/2)$, $R_{-M}(1-p/2)$ та $S_{-M}(p/2)$, $S_{-M}(1-p/2)$. Точки $R_M(p/2)$, $R_M(1/2)$, $R_M(1-p/2)$ та $S_{-M}(p/2)$, $S_M(1/2)$, $S_{-M}(1-p/2)$ задають дві параболи. Кожна парабола і відповідні лінії перетинаються зліва. Середнє арифметичне від x-координат обох перетинів дозволяє нам оцінити невідому довжину p повідомлення.

Для того, щоб уникнути затратного за часом статистичного оцінювання серединних точок $R_M(1/2)$ і $S_M(1/2)$ і, одночасно, зробити оцінку довжини повідомлення елегантніше, зробимо два додаткових припущення: (А) — точка перетину кривих R_M і R_{-M} має однакову x-координату, як і точки перетину кривих S_M і S_{-M}. Це суттєво сильніше припущення, ніж припущення, зроблене для залежності (2). (Б) — криві RM і SM перетинаються для $m = 50$ %, або $R_M(1/2) = S_M(1/2)$.

Автори винаходу [6] перевірили ці припущення експериментально для великої бази даних зображень з необробленими зображеннями у форматах BMP і JPEG, а також обробленими у форматі BMP. На основі емпіричних даних отримано просту формулу визначення довжини p секретного повідомлення.

Після зсуву і нормування осі x так, щоб $p/2$ стало нулем і $100-p/2$ стало 1, x-координата точки перетину — це корінь із такого квадратного рівняння:

$$2(d_1 + d_0)x^2 + (d_{-0} - d_1 - 3d_0)x + d_0 - d_{-0} = 0,$$

де $d_0 = R_M(p/2) - S_M(p/2)$; $d_1 = R_M(1-p/2) - S_M(1-p/2)$;

$d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)\, d_{-1} = R_{-M}(1-p/2) - S_{-M}(1-p/2)$.

Довжина прихованого повідомлення p обчислюється з меншого за абсолютним значенням кореня рівняння:

$$p = x/(x-1/2).$$

Прямі лінії визначають кількість R і S груп в $p/2$ і $1-p/2$, а припущення, зроблені під час виведення залежностей (1) і (2), забезпечують достатню кількість обмежень для єдиного задання парабол і їхніх перетинів.

Фактори, що впливають на точність аналізу

Для дуже зашумлених і дрібнотекстурованих зображень різниця між кількістю регулярних і сингулярних груп контейнера мала. Відповідно, лінії в RS-діаграмі перетнуться під малим кутом і точність зменшиться.

Методика *RS*-стегоаналізу точніша для повідомлень, стего-біти яких випадково розміщені в площині стего-образу, ніж для повідомлень, вбудованих локально. Для того, щоб застосувати *RS*-аналіз у цьому випадку треба перейти до використання методики на базі ковзного вікна.

Іншим фактором, який впливає на точність оцінки довжини вбудованого повідомлення, є початкове зміщення. Випадкові варіації можуть призвести до того, що контейнер, який не містить прихованих повідомлень, буде показувати наявність короткого повідомлення. Це початкове не нульове зміщення може бути як позитивним, так і негативним і встановлює теоретичні межі точності стеганоаналітичної методики, поданої у винаході. Автори винаходу протестували це початкове зміщення для набору з 331 монохромного JPEG зображення, які мають гауссівський розподіл з

дисперсією 0,5 %. Для менших зображень є тенденція збільшення варіації початкового зміщення, оскільки вони мають меншу кількість RS-груп. Сканування напівтонових і зашумлених зображень показує вищі варіації зміщення. З іншого боку, зміщення дуже мале для JPEG-зображень, не стиснутих зображень, отриманих з цифрових камер і результатів сканування з високим розрізненням.

У результаті досліджень, проведених співробітниками ЦТОС ІК над 3500 зображеннями (пустими контейнерами), які доступні в Інтернеті, виявилось, що відсоток хибного визначення обсягу прихованого повідомлення для них вищий, ніж указаний авторами патенту для фотографій із цифрових камер і сканерів.

Це пов'язано з тим, що під час підготовки до друку виконано обробку таких зображень, які включають високочастотну фільтрацію, підвищення яскравості і контрасту, вирівнювання значень гістограми і т. п. операції, які підвищують візуальну якість зображення. Це супроводжується збільшенням сингулярних груп у контейнері.

Також помічено нерівномірне зашумлення по каналах для кольорових зображень. Ступінь зашумлення блакитного каналу в два—три рази, а іноді в десять разів більше за рівень шуму у червоному і зеленому каналах. Крім того, рівень шуму у зеленому каналі для звичайних фотографій в два—три рази вищий за рівень шуму у червоному, але для зимових пейзажів спостерігається обернена закономірність. Таким чином, рівень зашумлення каналу залежить від кількості й абсолютного значення байт.

У табл. 2 наведено типові значення розмірів виявлених повідомлень у пустих контейнерах для зображень різних типів.

Таблиця 2

Типові відсотки значень розмірів виявлених повідомлень RS-аналізом

Тип зображення	Хибно визначена довжина повідомлення у відсотках від об'єму контейнера
Фотографії, скановані зображення	≈ 1 %
Зображення з Інтернету, підготовлені до друку	≈ 15 … 20 %
Дрібнотекстуровані зображення, високодеталізовані зображення	≈ 30 … 100 %

Перелічені фактори суттєво знижують ймовірність виявлення прихованих даних навіть для класичної НЗБ-стеганографії, якщо відповідні програми використовуються підготовленими особами.

Розглянемо новий **стеганографічний алгоритм кодування пар байтів** (КПБ).

Нехай байти значенням Z відповідають нульовому стего-біту, а байти значенням $Z + 1$ — одиничному стего-біту. Тоді двійкову послідовність стего-біт секретного повідомлення можна відобразити на множину пар байтів, які не мають спільних елементів. Причому значення байтів будуть відповідати нульовим і одиничним стего-бітам, а їхні індекси відносно початку масиву — чергуванню стего-бітів. В узагальненому вигляді алгоритму між парами біт можна встановити зміщення D. Для найпростішого випадку $D = 1$, проте його можна встановлювати як цілим числом $1 < D < 255$, так і змінювати за алгоритмом. Таким чином, $Z + D \rightarrow 0_2$, $Z + 1 + D \rightarrow 1_2$, де $Z = 0, 1, \ldots 255$; $D = 1, 2, \ldots 254$.

У роботі [7] показано, що перевертання $0 \leftrightarrow 1$, $2 \leftrightarrow 3$, …, $254 \leftrightarrow 255$; $1 \leftrightarrow 2$, $3 \leftrightarrow 4$, …, $253 \leftrightarrow 254$ відповідають внесенню в НЗБ контейнера прихованого повідомлення.

Тобто, базою в будові концепції для створення ефективнішого методу стеганографічного приховування інформації є внесення змін, що не будуть підпадати під вказане вище перевертання. Очевидно, що таке приховування інформації буде трактуватись *RS*-аналізом як шум.

З урахуванням цього авторами статті (науковими співробітниками ЦТОС ІК) проведено чисельні експерименти з різними значеннями перевертання, що й підтвердили вищенаведене припущення.

Якщо взяти за 100 % ємності контейнера повне його заповнення за методом НЗБ стеганографії, коли в кожному байті міститься один стего-біт, то із заповненням контейнера від 1 до 100 % отримаємо відповідну оцінку за методом *RS*-аналізу. Проте у разі заповнення за алгоритмами, що відповідають новій концепції, RS-аналіз видає значення, яке приблизно дорівнює значенню для пустого контейнера. Зазначимо, що таке вбудовування повідомлень також не виявляє такий метод стеганоаналізу як Sample Pairs [5]. Таким чином, *RS*-аналіз у своєму запатентованому вигляді не

розпізнає внесення стего-бітів за, по суті, модифікованим НЗБ-стеганографічним алгоритмом, що розробляється авторами роботи.

На сьогодні, усі науково-дослідні результати з розробки нової концепції [9] інтегруються для створення найбільш універсального та ефективного алгоритму стеганографічного приховування інформації, що буде обходити *RS*-стегоаналіз. Якщо розроблені методи та алгоритми підтвердять свою ефективність, то вони будуть запатентовані та описані в подальших публікаціях на цю тему.

Висновки

1. Запропоновано концепцію побудови нового методу стеганографічного приховування інформації, яка дозволяє уникнути виявлення методами стеганоаналізу, побудованими на базі дуальної статистики.

2. Наведено аналіз переваг і недоліків RS-стеганоаналізу.

3. Подано дані щодо особливостей аналізу кольорових каналів фотографій зображень, підготовлених до друку, у яких спостерігається помилкове виявлення повідомлень великої довжини.

СПИСОК ЛІТЕРАТУРИ

1. Корольов В. Ю. Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора / В. Ю. Корольов, В. В. Поліновський, О. В. Малікова // Вісник Хмельницького національного університету. — 2008. — № 3.— С. 175—181.

2. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с. (Серия «Аспекты защиты»)

3. Хорошко В. О. Основи комп'ютерної стеганографії : навч. посіб. / В. О. Хорошко, Л. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук. — Вінниця : ВДТУ, 2003. — 143 с.

4. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : «МК-Пресс», 2006. — 288 с., ил.

5. Digital Watermarking and Steganography / I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker, Morgan Kaufmann Publishers, second edition, 2008.

6. United States Reissued Patent US RE40,477 E Reliable Detection of LSB Steganography in Color and Grayscale Images. Inventors: Jessica Fridrich, Miroslav Goljan. — Sep. 2, 2008.

7. Fridrich J., Goljan M., Du R. Lossless Data Embedding — New Paradigm in Digital Watermarking, Special Issue on Emerging Applications of Multimedia Data Hiding, Vol. 2002, No. 2, February 2002, P. 185—196.

8. Зацеркляний М. М. Дослідження методу RS-стеганоаналізу / М. М. Зацеркляний, Г. С. Кириченко // Вісник НТУ «ХПІ». Тематичний випуск: Інформатика і моделювання. — Харків : НТУ «ХПІ». — 2008. — № 49. — С. 64—71.

9. Корольов В. Ю. Стеганографічна персоналізація інформації на базі ПК / В. Ю. Корольов, В. В. Поліновський, В. А. Герасименко // Вісті Академії інженерних наук України. — 2009. — № 2(39).— С. 18 — 24.

Рекомендована кафедрою телекомунікаційних систем та телебачення

Надійшла до редакції 27.01.10
Рекомендована до друку 01.11.10

Корольов Вячеслав Юрійович — завідувач відділом проблем моделювання пристроїв таймерної обчислювальної техніки;

Поліновський Вячеслав Васильович – старший науковий співробітник, ***Герасименко Вячеслав Анатолійович*** — молодший науковий співробітник.

Центр таймерних обчислювальних систем Інституту кібернетики ім. В. М. Глушкова НАН України